Juice Shop Bug List and Report

Bug ID: JUICE-AUTH-001

Title: Weak Password Authentication Allows Unauthorized Admin Access

Priority: P1 (Highest)
Severity: Critical

Reported By: Rahul Srivastava
Reported Date: January 5, 2025

Product: OWASP Juice Shop
Version: [Application Version]

Component: Authentication System

Environment:

- Application URL: https://juice-shop.herokuapp.com/#/
- Browser: Chrome Version 131.0.
- OS: Windows

Description:
The application's authentication system accepts weak passwords for administrator accounts, allowing unauthorized access through simple password guessing.

Precondition:

- Application is accessible
- Admin email is visible in product reviews section
- Login page is accessible

Steps to Reproduce:

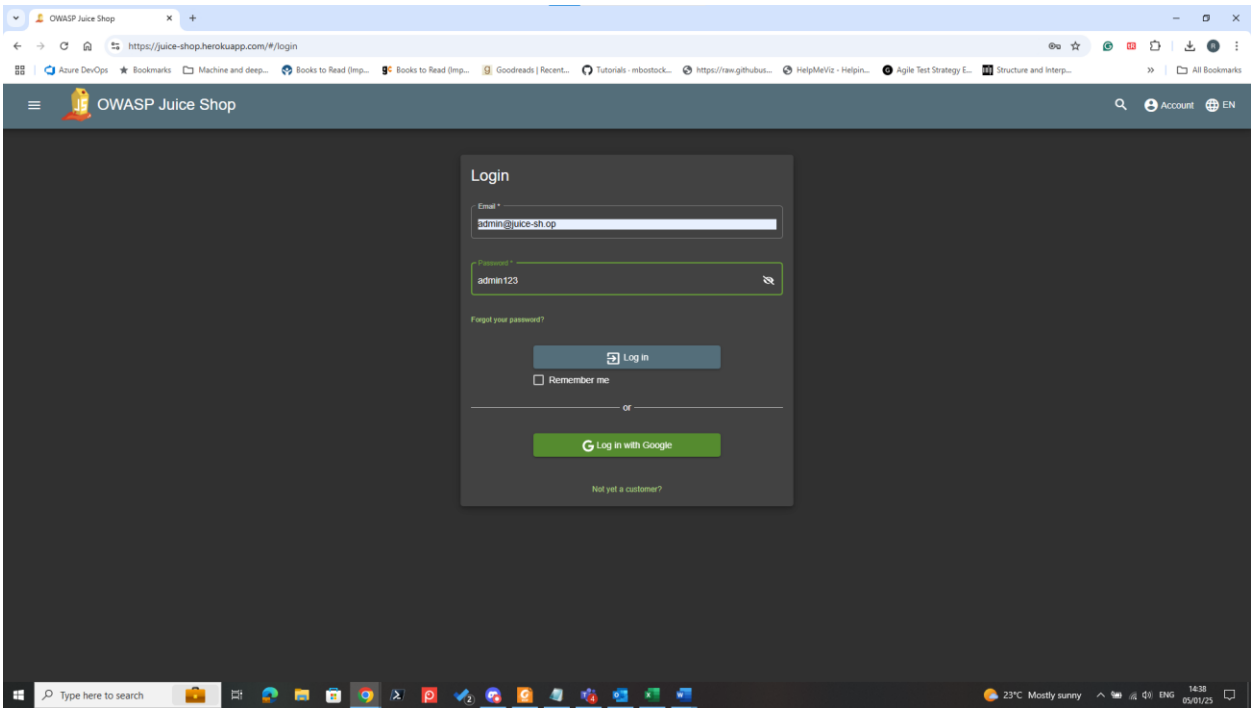
1. Navigate to first product's review section
2. Identify admin email address (admin@juice-sh.op)
3. Go to login page
4. Enter email: admin@juice-sh.op
5. Enter password: admin123

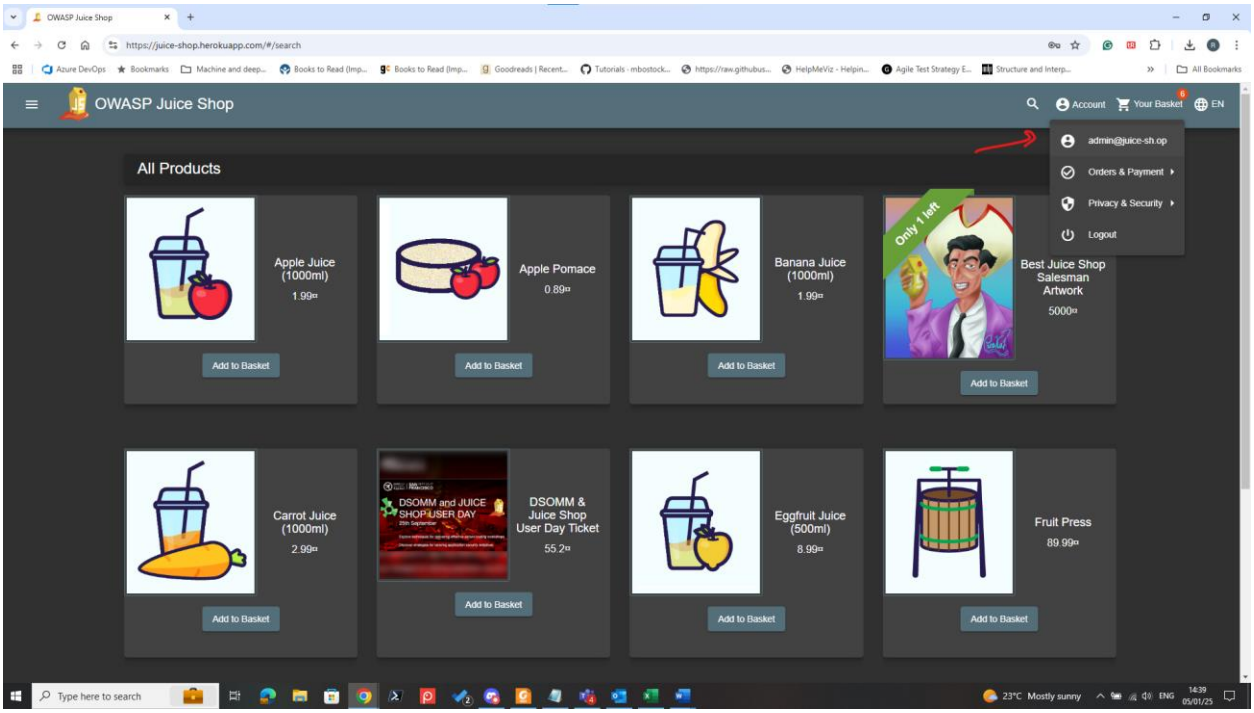
6. Click Login button

Expected Result: The system should reject weak passwords and prevent unauthorized access to administrative accounts.

Actual Result: Successfully logged in as administrator using a weak, easily guessable password.

Screenshot/Video:





Defect Type: Security

Status: New

Reproducibility: Always (100%)

Business Impact:

- Unauthorized access to admin functions
- Potential data breach
- Security compliance violations
- Reputational damage

Bug ID: JUICE-SEC-002

Title: SQL Injection Authentication Bypass Using OR 1=1 Payload

Priority: P1 (Highest)
Severity: Critical

Reported By: Rahul Srivastava
Reported Date: January 5, 2025

Product: OWASP Juice Shop
Version: [Application Version]

Component: Authentication System - Login Form

Description:
The login form is vulnerable to SQL injection, allowing authentication bypass using a basic SQL injection payload. The application accepts the input "' OR 1=1--" in the password field, resulting in successful authentication without valid credentials.

Steps to Reproduce:

1. Navigate to the login page via Account dropdown
2. Enter the following value in the email field: ' OR 1=1--
3. Enter any value in the password field
4. Click the Login button

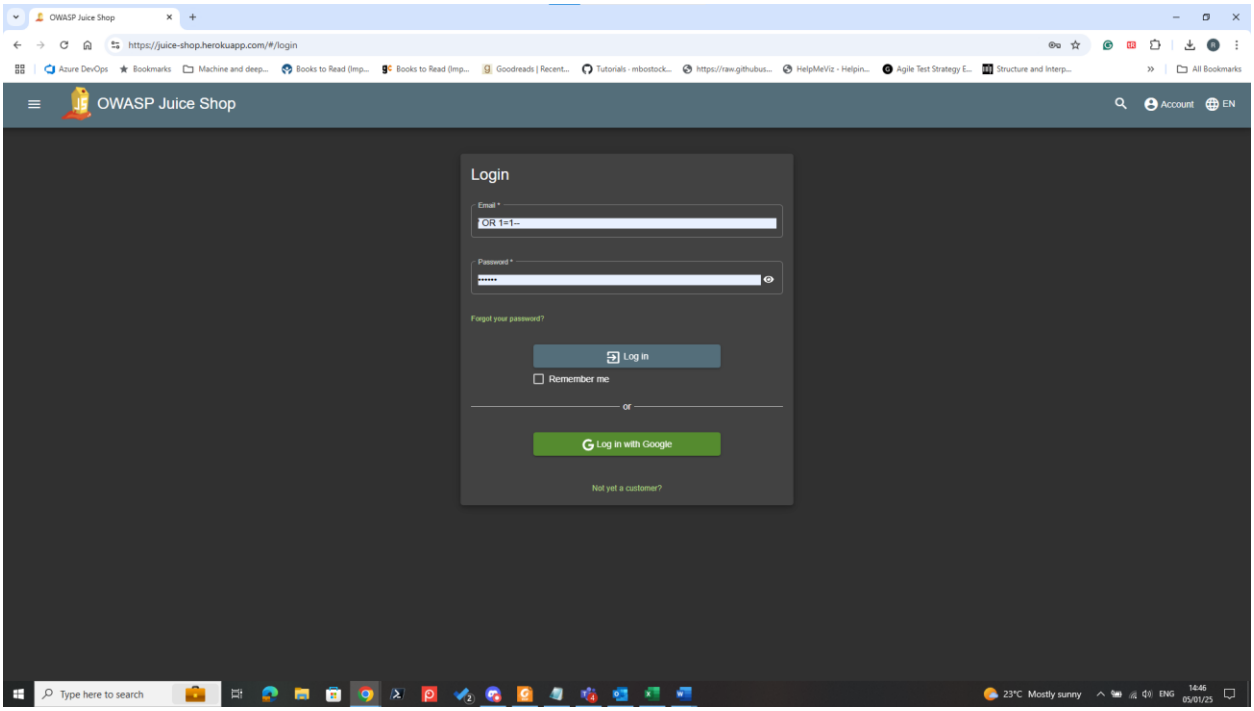
Expected Result:

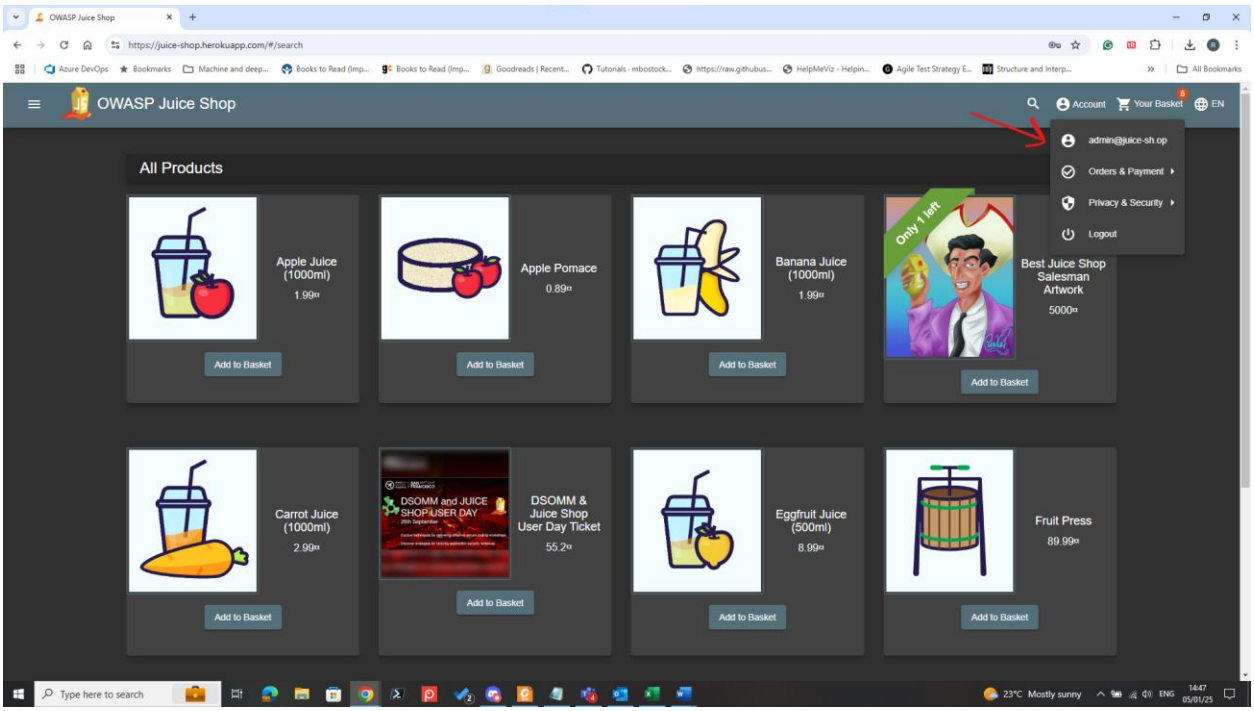
- The application should reject the SQL injection attempt
- Authentication should fail
- An error message about invalid credentials should be displayed

Actual Result:

- Authentication is successfully bypassed
- Access is granted to the application
- No error messages are displayed
- User is logged into the system

Screenshots:





Defect Type: Security Vulnerability

Status: New

Reproducibility: Always (100%)

Impact:

- Unauthorized users can gain access to the application
- Authentication system completely bypassed
- No valid credentials required
- Potential access to sensitive user data

Root Cause:

1. Lack of input validation
2. Lack of prepared statements
3. Direct injection of user input into SQL query
4. Missing input sanitization

Payload Analysis: ' OR 1=1--

- Single quote (') : Breaks out of the SQL string
- OR 1=1 : Creates a condition that always evaluates to true
- -- : Comments out the remainder of the SQL query

Bug ID: JUICE-SEC-004

Title: SQL Injection in Email Field Allows Authentication Bypass

Priority: P1 (Highest)
Severity: Critical

Reported By: [Tester Name]
Reported Date: January 5, 2025

Product: OWASP Juice Shop
Version: [Application Version] **Component**: Authentication System - Login Form (Email Field)

Description:
The email field in the login form is vulnerable to SQL injection that allows targeted account access. Unlike generic authentication bypass payloads, this vulnerability enables unauthorized access to a specific user account (in this case, Bender's account) when using their email address with a SQL injection payload, bypassing password verification.

Precondition:

- Access to application
- Known user email (bender@juice-sh.op) obtained from product reviews

Steps to Reproduce:

1. Navigate to the login page via Account dropdown
2. Enter the following in email field: bender@juice-sh.op'--
3. Enter any random value in password field
4. Click the Login button

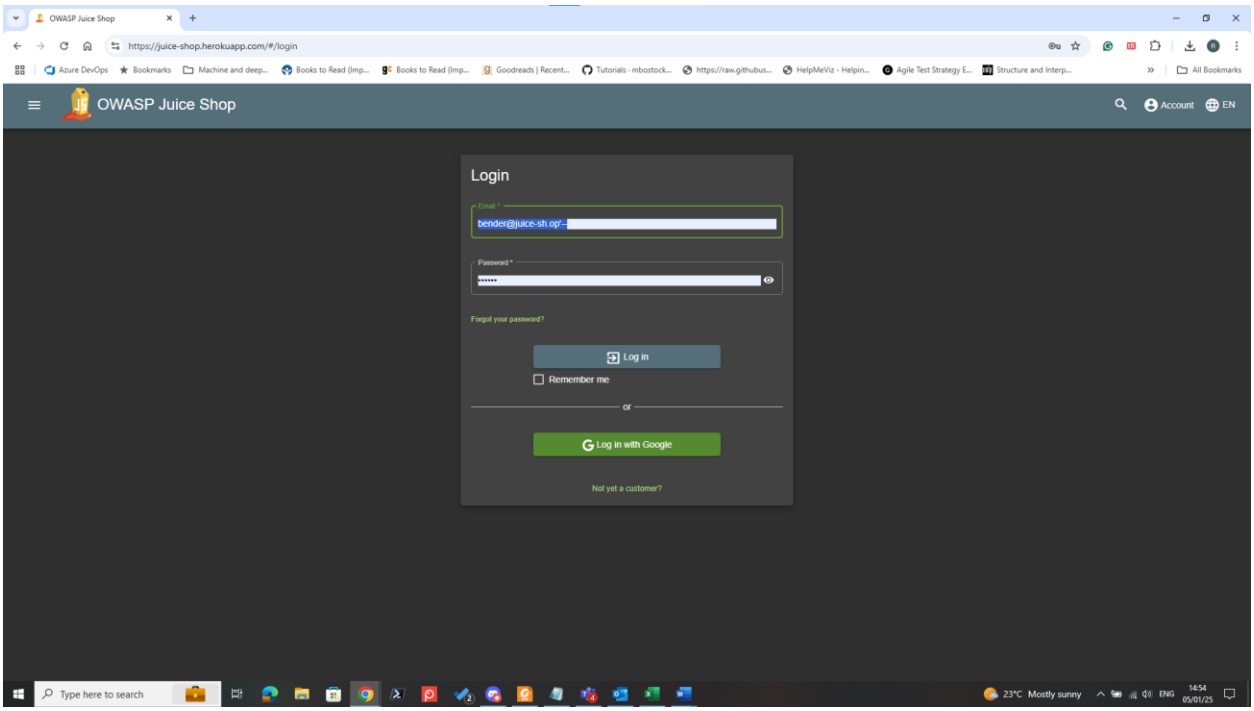
Expected Result:

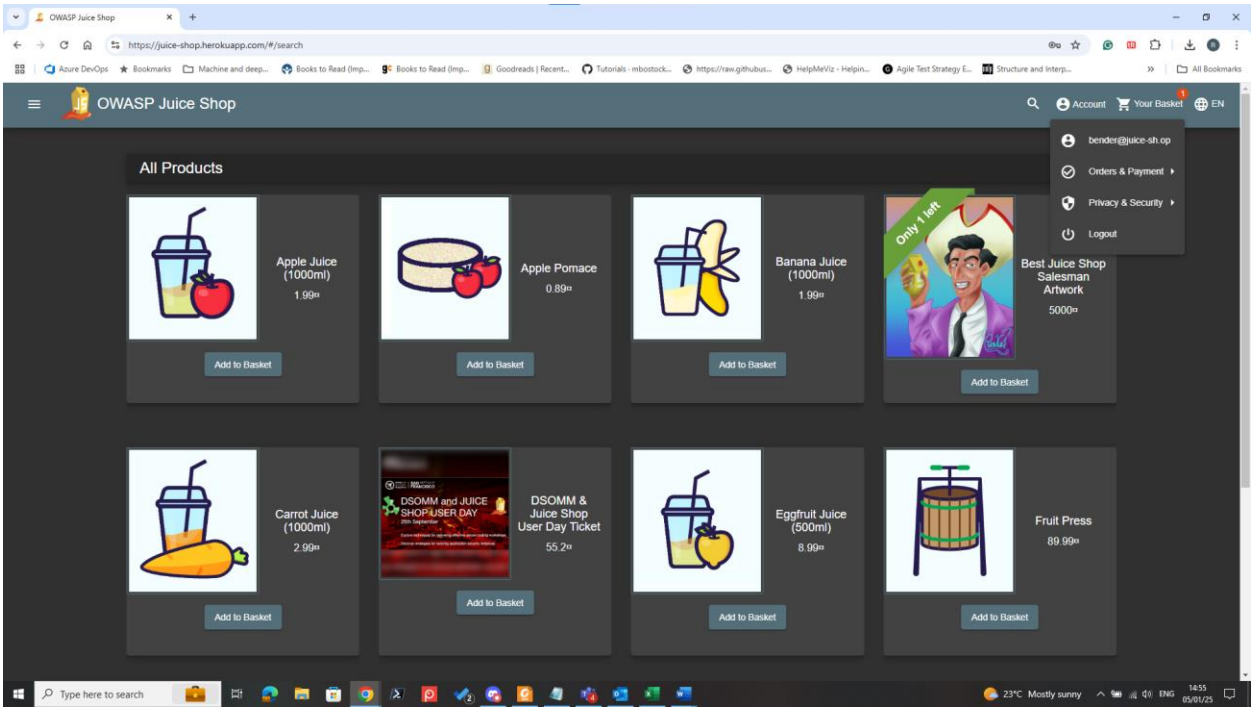
- The application should reject the malformed email address
- Authentication should fail
- System should display invalid credentials error

Actual Result:

- Authentication successful
- Successfully logged in as user 'bender'
- System accepts SQL injection in email field
- Password validation is bypassed

Screenshots:





Defect Type: Security Vulnerability

Status: New

Reproducibility: Always (100%)

Impact:

- Targeted unauthorized access to specific user accounts
- Ability to impersonate known users
- Complete bypass of password authentication
- Access to user-specific data and functionality
- Potential for targeted theft of personal information
- Ability to perform actions as the compromised user

Technical Analysis: Payload breakdown: bender@juice-sh.op'--

- Valid email address: bender@juice-sh.op
- Single quote ('): Closes the SQL string
- Double dash (--): Comments out remainder of query
- No password verification required

Root Cause:

1. Lack of input validation on email field
2. No email format enforcement
3. Direct inclusion of user input in SQL query
4. Missing prepared statements
5. Inadequate input sanitization